A CRITICAL REVIEW OF CYBERSECURITY EDUCATION IN THE UNITED STATES

Abstract

by James Laurence Crabb, M.S.
Washington State University
December 2023

Chair: Assefaw Gebremedhin

Cybersecurity is a critical field in modern society as compromised data or network infrastructure directly impact privacy, livelihood, and safety. Professionals in the cybersecurity field must be able to respond effectively to attacks being carried out by adversaries of varying experience level. In order to ensure that the cybersecurity workforce in the United States stays ahead of the competition, we must periodically review how we train our workforce, with a critical eye for areas that need improvement. The goal of this thesis is to perform such a review, identify trends in how cybersecurity professionals in the U.S. are being educated and trained, and suggest improvements.

The thesis makes four major contributions. The first is an analysis of top cybersecurity programs in the United States. A sample of one hundred institutions designated by the National Security Agency as Centers of Academic Excellence in Cybersecurity was examined to understand how their programs are structured and administered. Curricula varied widely in the proportion of cybersecurity-specific courses required by the programs. This is a strength because it includes a wider variety of programs in the certification process, and it is a weakness because it requires individual programs to identify and clearly communicate areas within cybersecurity that they target.

The second contribution is an analysis of contemporary research on cybersecurity education. Specifically, an investigation of fifty research papers on cybersecurity education was conducted to identify major topics of recent research. The results show a strong focus on identifying instructional content and developing educational tools while simultaneously indicating a shortage of research into rigorous evaluation of the instructional approaches.

The third contribution pertains to curricular framework analysis. Cybersecurity curricula are also shaped by the recommendations of groups such as the National Security Agency and the National Institute of Standards and Technology. Using Bloom's Revised Taxonomy, a well-known tool from educational psychology, three cybersecurity education frameworks were compared by determining which cognitive levels were associated with their learning outcomes. This revealed a gap between industry requirements and academic goals. To bridge this gap, academic recommendations should incorporate learning outcomes that target higher cognitive levels, or in other words, promote more active application of learned knowledge.

Finally, Washington State University's new cybersecurity degree program was evaluated for alignment with the National Initiative for Cybersecurity Education's (NICE) Workforce Framework for Cybersecurity and correspondence of the program to ABET requirements. By comparing the requirements of select work roles included in the NICE framework with the learning outcomes of courses required by the degree program, we can identify which jobs this program best prepares its graduates for. Performing such an evaluation is useful to both students and employers looking for cybersecurity programs that are the most relevant to them.